**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF NEW YORK**

| | |
|---|---|
| DONALD SISSON, *individually and on behalf of all others similarly situated*,<br><br>Plaintiff,<br><br>v.<br><br>MONRO, INC.,<br><br>Defendant. | Case No. 6:25-cv-06166<br><br>**JURY TRIAL DEMANDED** |

# CLASS ACTION COMPLAINT

Plaintiff Donald Sisson ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Monro, Inc. ("Defendant"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

## NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") protected health information ("PHI"), including names, Social Security numbers, addresses, dates of birth, ID numbers, and certain health information (collectively, "Private Information").[1]

2. In November 2024, hackers targeted and accessed an employee's email account and stole Plaintiff's and Class Members' sensitive, confidential Private Information stored therein, causing widespread injuries to Plaintiff and Class Members (the "Data Breach").

3. Defendant is an automotive and tire dealer that services clients across the United

[1] *See* the "Notice Letter". A sample copy is available at https://oag.ca.gov/ecrime/databreach/reports/sb24-600257

States.[2]

4. Plaintiff and Class Members are current and former employees of Defendant's who, in order to obtain employment from Defendant, was required to entrust Defendant with their sensitive, non-public Private Information. Defendant could not perform its operations or provide its services without collecting Plaintiff's and Class Members' Private Information and retains it for many years, at least, even after the employee relationship has ended.

5. Businesses like Defendant that handle Private Information owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their Private Information.

6. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard their Private Information it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, which failures allowed criminal hackers to access and steal employees' Private Information from Defendant.

7. According to Defendant's notice of the Data Breach, in late November 2024, Defendant detected unusual activity on an employee's email account. The ensuing investigation revealed that during the event an unknown, unidentified hacker accessed and exfiltrated files containing Plaintiff's and Class Members' Private Information.

[2] https://corporate.monro.com/company/ (last visited Mar. 27, 2025).

8. Although the Data Breach took place, at latest, prior to November 2024, Defendant failed to notify affected individuals that their Private Information was compromised until approximately March 21, 2025—diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address the increased, imminent risk of identity theft and other harms the Data Breach caused.

9. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its employees' sensitive data.

10. Defendant maintained the Private Information in a reckless manner. In particular, Private Information was maintained on and/or accessible from Defendant's network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

11. Hackers targeted and obtained Plaintiff's and Class Members' Private Information from Defendant's network because of the data's value in exploiting and stealing identities. As a direct and proximate result of Defendants' inadequate data security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information has been accessed by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

12. The harm resulting from a cyberattack like this Data Breach manifests in numerous

ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

13. As a result of the Data Breach, Plaintiff and Class Members suffered and will continue to suffer concrete injuries in fact, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. To recover from Defendant for these harms, Plaintiff, on his own behalf and on behalf of the Class as defined herein, brings claims for negligence/negligence *per se*, breach of implied contract, and invasion of privacy, to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information in its care.

15. Plaintiff and Class Members seek damages and equitable relief requiring Defendant to (a) disclose the full nature of the Data Breach and types of Private Information exposed; (b) implement data security practices to reasonably guard against future breaches; and (c) provide, at Defendant's expense, all Data Breach victims with lifetime identity theft protection services.

## PARTIES

16. Plaintiff Donald Sisson is an adult individual who at all relevant times has been a citizen and resident of Rochester, New York.

17. Defendant Monro, Inc. is a New York corporation with its principal place of business at 200 Holleder Pkwy, Rochester, New York 14615.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendant, as the Data Breach affected Class Members in multiple states.

19. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in New York and Defendant engaged in substantial activity in New York.

20. This District is an appropriate venue because it is the District where Defendant resides and where a substantial part of the events and omissions giving rise to the claims occurred.

## FACTUAL BACKGROUND

### A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for Private Information it Collected and Maintained.

21. Defendant is an automotive and tire part supplier that operates across the United States.

22. Plaintiff and Class Members are current and employees of Defendant who worked for Defendant in or prior to November 2024.

23. As a condition and in exchange for receiving employment from Defendant, Defendant's employees, including Plaintiff and Class Members, were required to entrust

Defendant with highly sensitive Private Information, including their names, Social Security numbers, addresses, dates of birth, and health information.

24. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

25. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

26. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive Private Information belonging to Plaintiff and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

27. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose Private Information was compromised, as well as intrusion into those individuals' highly private medical information.

28. Upon information and belief, Defendant made promises and representations to its employees, including Plaintiff and Class Members, that the Private Information collected from them as a condition of employment from Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it were no longer required to maintain it.

29. Plaintiff and Class Members relied on these promises from Defendant, a sophisticated business entity, to implement reasonable practices to keep their sensitive Private Information confidential and securely maintained, to use this information for necessary purposes

only and make only authorized disclosures of this information, and to delete Private Information from Defendant's systems when no longer necessary for its legitimate business purposes.

30. But for Defendant's promises to keep Plaintiff's and Class Members' Private Information secure and confidential, Plaintiff and Class Members would not have sought employment from or entrusted their Private Information to Defendant.

31. Based on the foregoing representations and warranties and to obtain employment from Defendant, Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

32. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

33. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its operations.

34. By obtaining, using, and benefiting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting that Private Information from unauthorized access and disclosure.

35. Defendant had and has a duty to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks, and train employees with access to use adequate cybersecurity measures.

36. Additionally, Defendant had and has obligations created by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), common law, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure. Defendant failed to do so.

**B. Defendant Failed to Adequately Safeguard Plaintiff's and Class Member's Private Information, resulting in the Data Breach.**

37. On or about March 21, 2025, Defendant began sending Plaintiff and other Data Breach victims letters informing them of the Data Breach ("Notice Letters").

38. The Notice Letters generally inform as follows, in part:

> WHAT HAPPENED: In late 2024, Monro became are of suspicious activity relating to an employee's electronic mailbox. Once we became aware of this activity, an investigation was undertaken that ultimately confirmed that an unknown and unauthorized actor accessed the employee's mailbox and selected files for a limited period of time in late November of last year.
>
> WHAT INFORMATION WAS INVOLVED: A comprehensive review of the impacted mailbox continued through on or about January 28, 2025, which revealed that certain personal information, including your name and social security number, could have been affected. Other data fields at issue could have included address, date of birth, ID number, and certain health information collected from employees, like accident history. Although we do not know what, if any, personal information may have been viewed by the unauthorized third party, Monro is providing this notice as a conservative measure.[3]

39. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

[3] Notice Letter.

40. Thus, Defendant's purported 'disclosure' amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

41. To make matters worse, although the Data Breach occurred in late 2024, Defendant waited until March 21, 2025 before notifying the public or affected individuals about it, diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address harms resulting from their Private Information's unauthorized disclosure.

42. Plaintiff's and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiff's and Class Members' Private Information from Defendant's network systems, where they were kept without adequate safeguards and in unencrypted form.

43. Defendant could have prevented this Data Breach by properly training personnel, securing account access through measures like multifactor authentication ("MFA") and recurring forced password resets, and/or securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information, but failed to do so.

44. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive Private Information it collected and maintained from Plaintiff and Class Members, such as MFA, standard monitoring and altering techniques, encryption, or deletion of information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network, access it through Defendant's employee email account, and exfiltrate files containing Plaintiff and Class Member's Private Information.

45. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information, using controls like limitations on personnel with access to sensitive data and requiring MFA for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access.

46. For example, if Defendant had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PHI and/or PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate malicious activity in Defendant's network systems for the period it took to carry out the Data Breach, including the reconnaissance necessary to identify where Defendant stored Private Information, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

47. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

48. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' Private Information, meaning Defendant had no effective means in place to ensure that cyberattacks were detected and prevented.

### C. Defendant Knew of the Risk of a Cyberattack because Entities in Possession of Private Information are Particularly Suspectable.

49. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and

securing such data.

50. Private Information of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the dark web.

51. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

52. Data thieves regularly target entities like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

53. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[4] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[5]

54. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June

[4] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last visited Mar. 27, 2025).
[5] *Id.*, at 15.

2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

55. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[6]

56. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[7]

57. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting entities like Defendant.

58. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

---

[6] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited Mar. 27, 2025).

[7] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last visited Mar. 27, 2025).

[8] *Id.*

59. As a business in possession of its employees' PHI, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being wrongfully disclosed to cybercriminals.

61. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to tens of thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

63. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

64. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

**D. Defendant was Required, but Failed to Comply with FTC Rules and Guidance.**

65. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9]

67. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

68. The FTC further recommends that companies not maintain confidential personal information, like Private Information, longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested

[9] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 27, 2025).
[10] *Id.*

methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

70. Such FTC enforcement actions include actions against entities like Defendant. *See, e.g., In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

71. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

72. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected

by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[11]

73. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

74. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

**E. Defendant Failed to Comply with Industry Standards.**

75. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

76. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[12]

[11] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[12] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last visited Mar. 27, 2025).

77. In addition, the NIST recommends certain practices to safeguard systems[13]:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

78. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing]

[13] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist- framework (last visited Mar. 27, 2025).

that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[14]

79. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

### F. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their Private Information.

80. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

81. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its

[14] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last visited Mar. 27, 2025).

possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

82. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner and act upon data security warnings and alerts in a timely fashion.

83. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

84. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

85. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

**G. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's conduct.**

86. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

87. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

88. Plaintiff and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its employees' Private Information.

89. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their Private Information ending up in criminals' possession, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

***The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing***

90. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

91. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*

92. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

93. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[17] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[18] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

94. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[19] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login

[17] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[18] *Id.*
[19] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

credentials, and Social Security numbers, dates of birth, and medical information.[20] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[21]

95. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' Private Information.

96. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

[20] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[21] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

98. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[22]

99. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[23]

100. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

[22] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Mar. 27, 2025).

101. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

102. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

103. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

104. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

105. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not

> reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[24]

106. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[25]

107. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[26] Yet, Defendant failed to rapidly report to Plaintiff and the Class that their Private Information was stolen.

108. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

109. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

110. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

---

[24] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited Mar. 27, 2025).
[25] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[26] *Id.*

***Loss of Time to Mitigate the Risk of Identify Theft and Fraud***

111. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

112. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record

113. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

114. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach.

115. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

116. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

***Diminished Value of Private Information***

117. Personal data like Private Information is a valuable property right.[28] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

118. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[29] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[30, 31]

---

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Mar. 27, 2025).

[28] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[29] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[30] https://datacoup.com/.

[31] https://digi.me/what-is-digime/.

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[32]

119. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

120. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

***Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary***

121. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

122. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

123. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for

[32] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[33] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

125. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

126. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

***Loss of Benefit of the Bargain***

127. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

128. When agreeing to provide their Private Information, which was a condition precedent to obtain employment from Defendant, Plaintiff and Class Members, as employees,

[33] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

understood and expected that Defendant would provide data security to protect the Private Information they were required to provide.

129. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

***Plaintiff's Experiences***

130. Plaintiff is a former employee of Defendant.

131. Upon information and belief, Plaintiff's Private Information was and continues to be stored and maintained in Defendant's network systems.

132. Plaintiff greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

133. Plaintiff would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

134. At the time of the Data Breach Defendant retained Plaintiff's Private Information in its network systems with inadequate data security, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

135. On or about March 21, 2025, Plaintiff received Defendant's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers accessed and acquired files containing Plaintiff's sensitive Private Information, including his name, date of birth, certain health information, ID number, and Social Security number.

136. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

137. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

138. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff's and Class Members' Private Information was targeted, accessed, and misused, including through publication and dissemination on the dark web.

139. Plaintiff further believes his Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

140. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress about his Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Defendant still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

141. Moreover, since the Data Breach Plaintiff has experienced suspicious spam calls and texts, using his Private Information compromised in the Data Breach, and believes this to be an attempt to secure additional information from or about him.

## CLASS ACTION ALLEGATIONS

142. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and 23(b).

143. Plaintiff proposes the following nationwide class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information may have been compromised in the Data Breach, including all individuals who received a Notice Letter (the "Class").

144. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

145. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

146. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Defendant has knowledge of the amount of individuals involved, evidenced by the Notice Letters Defendant sent to individuals whose Private Information was compromised in Data Breach.

147. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Class Members;

l. Whether Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

148. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

149. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

150. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

151. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member.

152. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

153. Likewise, particular issues are appropriate for certification pursuant to Federal Rule of Civil Procedure 23(c)(4) because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard employee Private Information; and

e. Whether adherence to FTC data security guidelines and/or measures recommended by data security experts would have reasonably prevented the Data Breach.

154. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified by Defendant.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE/NEGLIGENCE *PER SE*
### (On Behalf of Plaintiff and the Class)

155. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 154 above as if fully set forth herein.

156. Defendant required Plaintiff and Class Members to submit sensitive, confidential Private Information to Defendant as a condition receiving employment with Defendant.

157. Plaintiff and Class Members provided their Private Information to Defendant, including their names, Social Security numbers, dates of birth, addresses, and health information.

158. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

159. Defendant owed a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the Private Information it collected from them.

160. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendant.

161. Plaintiff and Class Members had no ability to protect their Private Information in Defendant's possession.

162. By collecting, transmitting, and storing Plaintiff's and Class Members' Private Information Defendant owed Plaintiff and Class Members a duty of care to use reasonable means to secure and safeguard their Private Information, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Defendant's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

163. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information.

164. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between it and its employees, which is recognized by laws and regulations

including but not limited to the FTC Act and the common law. Defendant was able to ensure its network servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiff and Class Members, yet it failed to do so.

165. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

166. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq*., Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

167. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices and procedures to safeguard Plaintiff's and Class Members' Private Information, and by failing to ensure the Private Information in its systems was encrypted and timely deleted when no longer needed.

168. Plaintiff's and Class Members' injuries resulting from the Data Breach were directly and indirectly caused by Defendant's violations of the FTC Act.

169. Plaintiff and Class Members are within Class Members of persons the FTC Act is intended to protect.

170. The type of harm that resulted from the Data Breach was the type of harm the FTC Act is intended to guard against.

171. Defendant's failure to comply with the FTC Act constitutes negligence *per se*.

172. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such Private Information.

173. Defendant breached its duties of care, and was grossly negligent, by acts of omission or commission, including by failing to use reasonable measures or even minimally reasonable measures to protect the Plaintiff's and Class Members' Private Information from unauthorized disclosure in this Data Breach.

174. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Maintaining and/or transmitting Plaintiff's and Class Members' Private Information in unencrypted and identifiable form;

c. Failing to implement data security measures, like adequate MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;

d. Failing to adequately train employees on proper cybersecurity protocols;

e. Failing to adequately monitor the security of its networks and systems;

f. Failure to periodically ensure its network system had plans in place to maintain reasonable data security safeguards;

g. Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and

h. Failing to adequately notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate damages.

175. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised because the malicious activity would have been prevented, or at least, identified and stopped before criminal hackers had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

176. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

177. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

178. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

179. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, as proven at trial.

180. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiff and all Class Members.

**COUNT II**
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiff and Class Members)**

181. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 154 above as if fully set forth herein.

182. On information and belief, Defendant entered into contracts with its employees to safeguard the Private Information that was to be provided to it.

183. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiff and Class Members, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and Class Members was the direct and primary objective of the contracting parties.

184. Defendant knew that if it were to breach these contracts with its employees, the employees, including Plaintiff and Class Members, would be harmed.

185. Defendant breached its contracts with its employees, and as a result Plaintiff and Class Members were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiff and Class Members regarding the breach.

186. As foreseen, Plaintiff and Class Members were harmed by Defendant's failure to use reasonable data security measures to store the Private Information Plaintiff and Class Members provided to Defendant and the failure to timely notify Plaintiff and Class Members, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

187. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

**COUNT III**
**INVASION OF PRIVACY/INSTRUSION UPON SECLUSION**
**(On behalf of Plaintiff and Class Members)**

188. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 154 above as if fully set forth herein.

189. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its possession against disclosure to unauthorized third parties.

190. Defendant owed a duty to its employees, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

191. Defendant failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons, criminal hackers, which on information and belief have made or imminently will make the Private Information publicly available and disseminated it to thousands of people, including through publishing the data on dark web leak sites, where cybercriminals go to find their next identity theft and extortion victims.

192. Defendant allowed unauthorized third parties access to and examination of the

Private Information of Plaintiff and Class Members, by way of Defendant's failure to protect the Private Information through reasonable data security measures.

193. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

194. The intrusion was into a place or thing, which was private and is entitled to be private—sensitive and confidential information including financial account numbers and Social Security numbers.

195. Plaintiff and Class Members disclosed their Private Information to Defendant as a condition of and in exchange for receiving employment, but privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and not be disclosed without their authorization, given Defendant's promises to that effect.

196. Subsequent to the intrusion, Defendant permitted Plaintiff's and Class Members' data to be accessed by hackers and, imminently if not already, published online to countless cybercriminals whose mission is to misuse such information through fraud and extortion.

197. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

198. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were insufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

199. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting it.

200. Defendant was aware of the potential of a data breach and failed to adequately safeguard its network systems or implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' Private Information to cybercriminals.

201. Because Defendant acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

202. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages including, without limitation: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

203. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and

used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff Donald Sisson, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent Class Members;

B. Awarding Plaintiff and Class Members damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and Class Members in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and Class Members;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding pre- and post-judgment interest, as provided by law;

H. Granting Plaintiff and Class Members leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiff and Class Members are entitled.

**JURY TRIAL DEMAND**

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: March 28, 2025

Respectfully submitted,

By: */s/ Randi Kassan*

Randi Kassan
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Telephone: 516-741-5600
rkassan@milberg.com

Gary M. Klinger (*Pro Hac Vice forthcoming)*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

*Counsel for Plaintiff and the Putative Class*